FORTINET
High Performance Network Security

FortiWLM

Release 8.3.3

FortiWLM 8.3.3 introduces features and enhancements as listed under the New Features section.

To ensure a secured Wi-Fi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware.

Getting Started with Upgrade

This section describes procedures for upgrading your Services Appliance.

Pre-requisites for Upgrade

Upgrade service appliances (SA / FWLM) before you initiate controller (FortiWLC-SD) upgrade.
While upgrading a Services Appliance with over 100 controllers, the controllers return to *active* state sequentially, one at a time. It may take up to 10 minutes or more for all controllers to become active.

Supported FortiWLM Upgrades

The following upgrade path is recommended.

From FortiWLM version…	To FortiWLM version
6.1-3-6/7.0-5-0	8.0-7-0
6.1-3-6/7.0-5-0/8.0-7-0	8.0-SR1-1
8.0-7-0/8.0-SR1-1	8.1-2-0
7.0-5-0/8.0-7-0/8.1-2-0	8.2.2
8.1-2-0/8.2.2	8.2.4
8.1-2-0/8.2.2	8.3.0
8.2.4/8.3.0	8.3.1
8.2.4/8.3.0/8.3.1	8.3.2
8.2.4/8.3.1/8.3.2	8.3.3

Supported FortiWLC-SD Releases

Network Manager Version	Supports Controllers with these FortiWLC-SD Versions
8.3.3	• 7.0-11-MR • 8.0-6-0-MR • 8.1-2-0 • 8.1-3-2MR • 8.2.4 • 8.2.7 • 8.3.0 • 8.3.1 • 8.3.2 • 8.3.3 • 8.4.0

Supported Hardware and Software

Hardware / Software	Supported Versions/Models
Service Assurance Manager	• AP110 • AP122 • AP320 • AP332 • AP433 • OAP433 • AP822 • AP832 • AP1020 • AP1014 • OAP832 • FAP-U421EV • FAP-U423EV • FAP-U321EV • FAP-U323EV • FAP-U422EV • FAP-U24JEV • FAP-U221EV • FAP-U223EV

Hardware / Software	Supported Versions/Models
Spectrum Manager	• AP332 • AP832 • PSM3x • AP1010 • AP1020 • FAP-U421EV • FAP-U423EV • FAP-U321EV • FAP-U323EV • FAP-U422EV • FAP-U24JEV • FAP-U221EV • FAP-U223EV
Controller Models	• FortiWLC-200D • FortiWLC-500D • FortiWLC-50D • FortiWLC-1000D • FortiWLC-3000D • MC1550 • MC1550-VE • MC3200 • MC3200-VE • MC4200 • MC4200-VE • FWC-VM-50 • FWC-VM-200 • FWC-VM-500 • FWC-VM-1000

	• FWC-VM-3000
Service Appliance	• FortiWLM-100D • FortiWLM-1000D • SA250 • SA2000 • SA2000-VE • AEC200 • AEC2000 • FWM-VM • Hyper-V • KVM
# Due to hardware limitations, High Availability is not supported in FortiWLM100D and SA250 appliances.	
Supported Browsers	• Internet Explorer 9 and later version *All the pages of EzRF will load under normal browser settings. Compatibility View Settings are not supported*. • Mozilla Firefox 32.0 • Google Chrome, version 34.0.1847.118 m

Application Visibility Policies

Application visibility policies in controllers running FortiWLC-SD 8.0 that is managed by FortiWLM 8.1 or later will be disabled. To continue using those policies, upgrade FortiWLC-SD to 8.1 or later.

FAP-U22xEV and FAP-U24J do not support application visibility, although FortiWLM 8.3.3 allows configuring it. FortiWLM 8.4.0 does not support configuring application visibility.

Upgrade Procedure

This procedure assumes that your Services Appliance is already installed on a network.

When upgrading from versions prior to FortiWLM 7.0, the DB is reset. It is therefore recommended that database backup should be taken before upgrade and restored after upgrade.

Upgrading via CLI

To upgrade a Services Appliance, perform the following steps:

1. Perform a complete Network Manager backup and copy the backup file to an external location. Use this if you run into a problem (Instructions for backing up the file can be found in the Maintenance chapter of the Network Manager User Guide.)
2. If you have SAM installed, disable all scheduled tests by performing the following steps:
    a. Select **Service Assurance**.
    b. From the left panel, select **Configure** > **Tests** > **Scheduled Tests**.
    c. Select the **Disable All** option and click **OK** continue.
3. Access the Services Appliance through SSH, using the administrative privilege.
4. If your appliance flash already contains three images, remove one of the older images using the `delete flash: <version number>` command.
5. Copy the file from the SCP server to your service appliance using the copy command:

```
sa# copy scp://user:password@server/path/meru-nm-<releaseVersion>-SA250-rpm.tar<space>.
```

6. Confirm the successful transfer of the image by displaying the current flash images using the `sh flash` command:

```
sa# sh flash
6.0-7-0 8.2-
1-0
```

7. Upgrade the service appliance:

```
sa# upgrade nms-server <Version>
```

This process installs new binaries and upgrades the stored data to the latest version. This process may take a few minutes and at the end of the upgrade the services appliance restarts. The time taken to upgrade, depends on the size of the data available on the services appliance.

8. Type the following command to confirm, if the installed software version is 8.3.3.

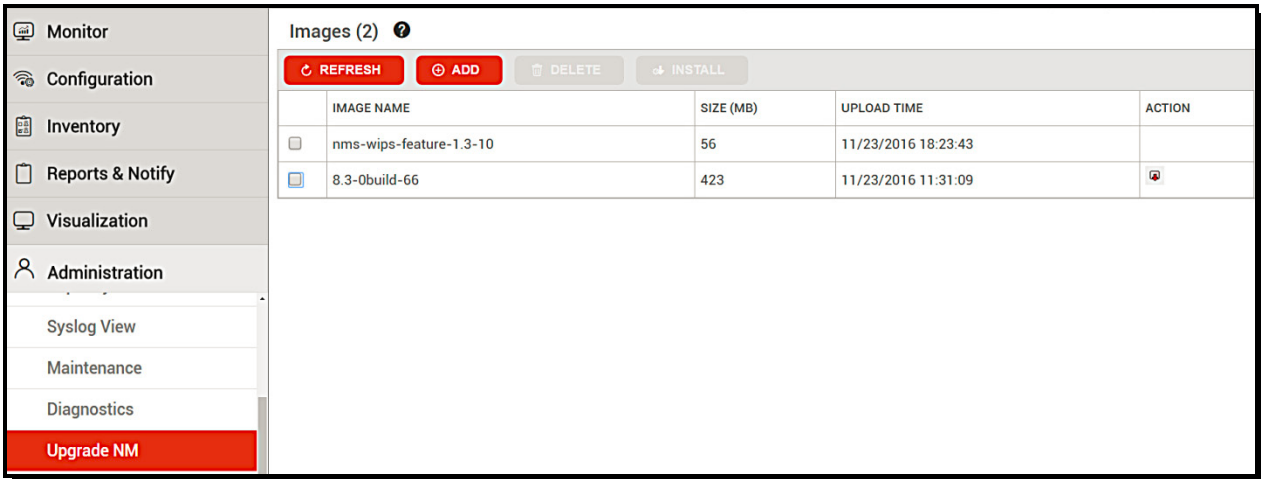
```
service appliance# sh nms
```

If the upgrade displays the "image integrity error," the service appliance image has been corrupted while uploading to Network Manager. Upload the new image again to the Network Manager service appliance and retry the upgrade. You can ignore the Security warning "Installing an unsigned upgrade package!" displayed by the upgrade command.

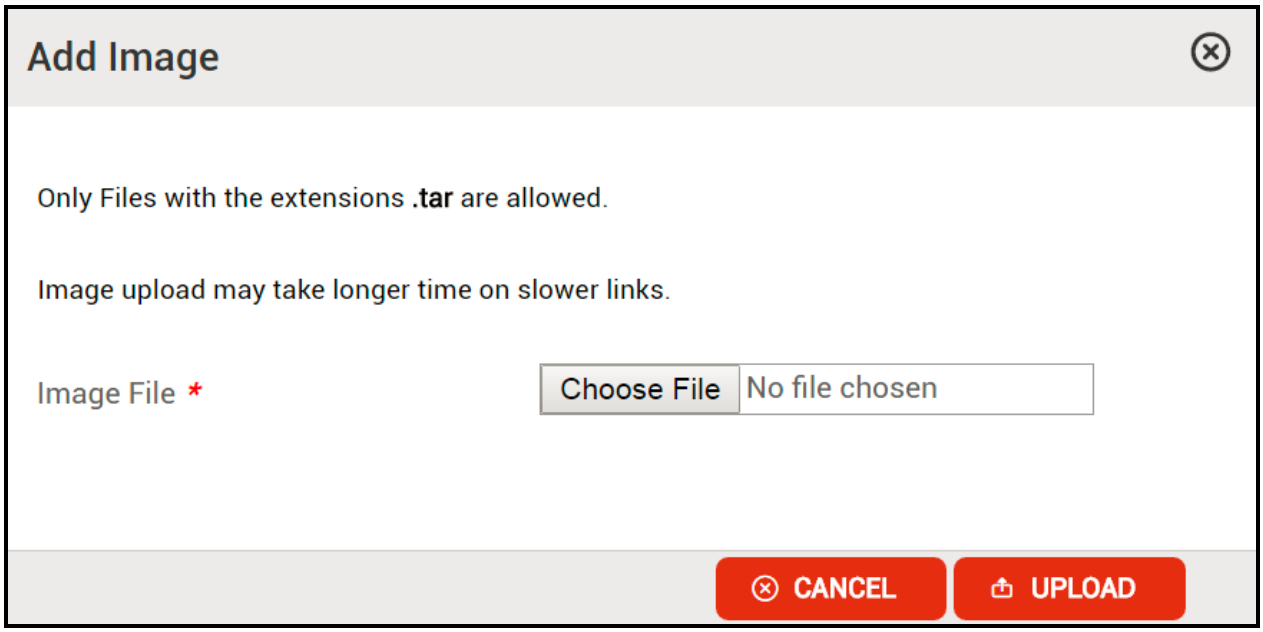
Upgrading via WebUI

The following procedure will guide you through the steps to upgrade your server from WebUI.

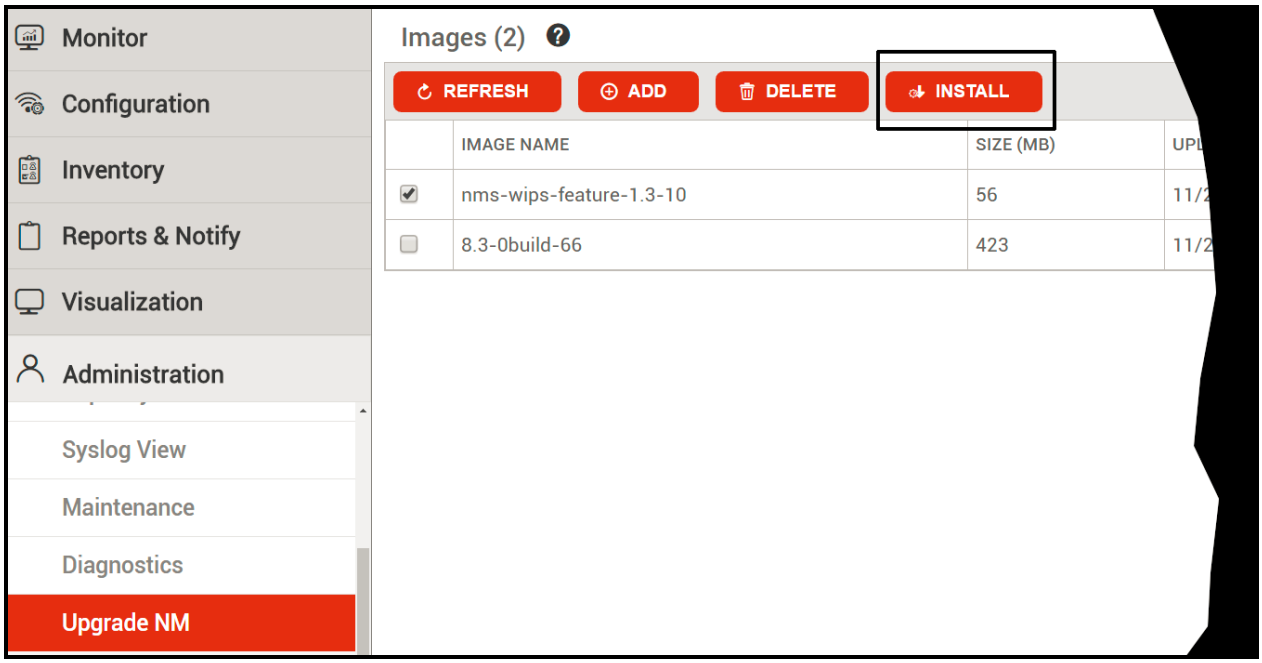
1. In the Network Manager WebUI, go to Administration > System Administration > Upgrade NM. By default, this page lists all the images copied to the server.



2. To upgrade your server to a different version than the ones listed, click **Add** to open the file selector window.



3. Select the image file from your computer or a network folder and click the **UPLOAD** button
4. After the upload is complete, select the version to install and click the **INSTALL** button to being the upgrade process.



During the upgrade process, do not click refresh or perform any operations on the server.

After the upgrade is complete, click Go the link to return to server operations.

- For a full upgrade, the server will restart after the upgrade process and return the page to server login prompt.
- For patch upgrade, the server will restart the process and return to the dashboard.

Post Upgrade Tasks

The following are optional post-upgrade tasks:

1. If you have not configured for automatic transfer of backup to a remote server, then follow the instructions for configuration in the **Administration** > **Maintenance** page.
2. If required, upload the license.

Install the application images downloaded in the pre-requisites for upgrade section using **`upgrade feature`** command.

Downgrade

Downgrading FortiWLM to a previous version is not supported. To go back to an older version of FortiWLM, you must do a fresh install of that version on your FortiWLM server.

Deploying FWLM VM on VMWare ESXi

This document describes the procedure to **deploy FWLM-VM as FWLM-VM-100D and FWLM-VM-1000D** on VMWare ESXi.
Note: Fortinet recommends VMWare ESXi version 6.5.

Supported Hardware Configuration

This table lists the supported configuration for FWLM-VM-100D and FWLM-VM-1000D.

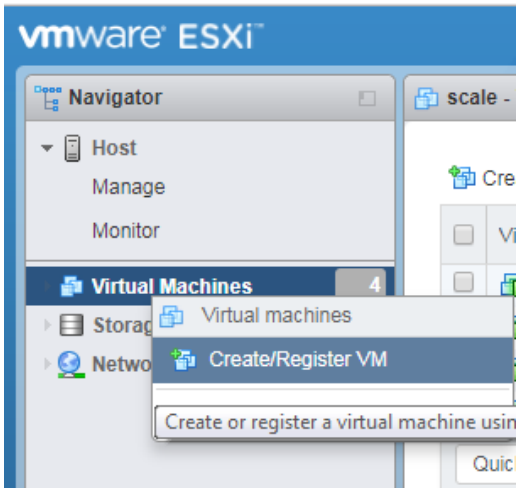
Configuration	FWLM-VM-100D	FWLM-VM-1000 D
Processor and Cores	Any Processor @ 2GHz or Higher. 4 Cores - 4 Threads	Any Processor @ 3.20GHz or Higher. 4 Cores - 8 Threads
Memory (DRAM)	4GB	16GB
Storage	1TB	2TB
Minimum Disk I/O	100MBps	100MBps
Network	1-4 1G RJ-45	1-4 1G RJ-45
Scale Numbers	AP: 1000 Stations: 5000 Spectrum Sensors: 100	AP: 15000 Stations: 75000 Spectrum Sensors: 750

Downloading the Virtual Machine Package File

You can download the virtual controller packages from the Fortinet Customer Support website. To access the support website you need a Fortinet Customer Support account. – **[URL required]**
The file name is, forti-wlm-x.x-xbuild-y-FWM-VM.ova, where x.x-x is the release version number. For example, 8.3.2.

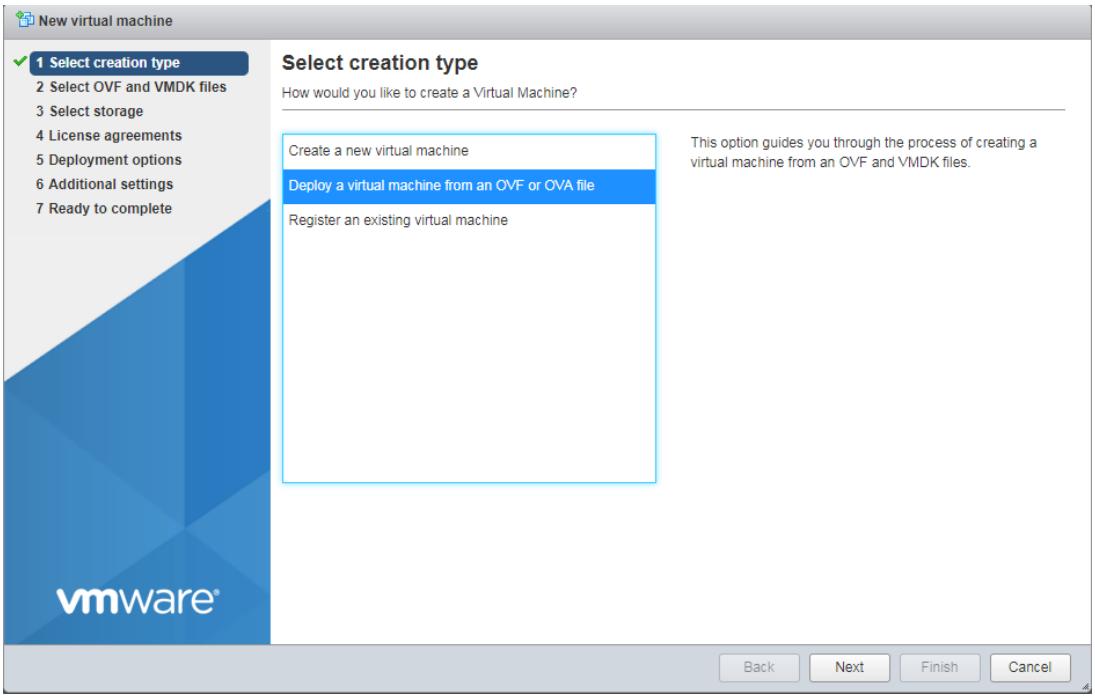
Creating the Virtual Machine

1. Open the VMWare ESXi console and navigate to **Virtual Machines < Create/Register VM**.

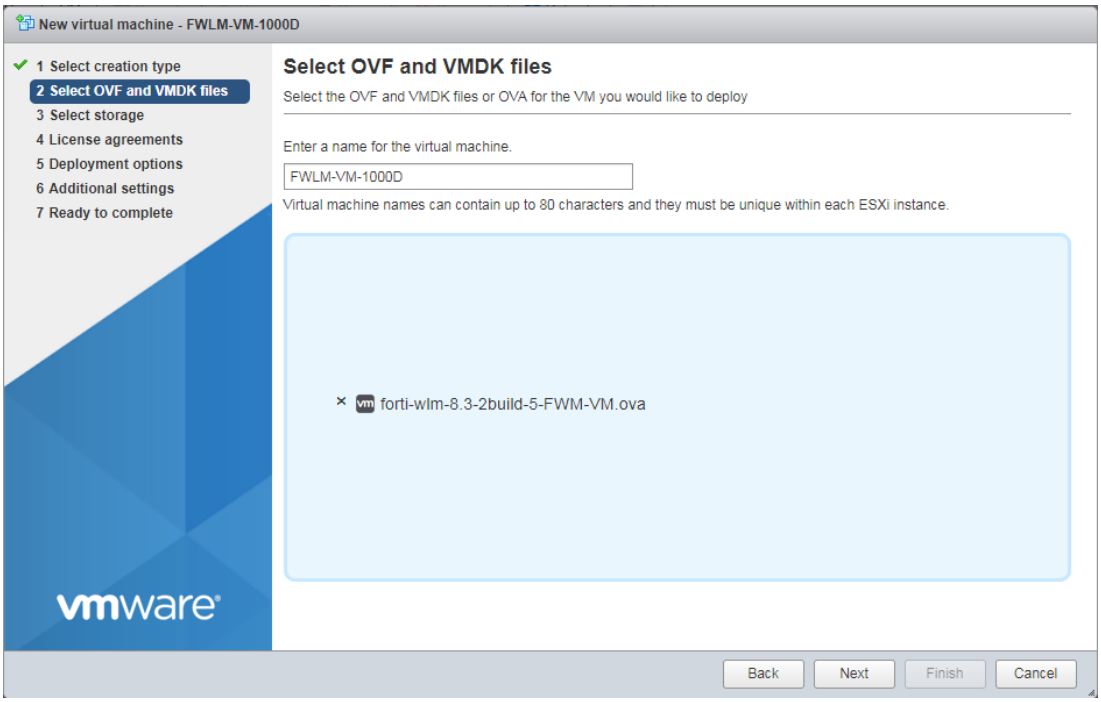


The **New Virtual Machine** wizard is displayed.

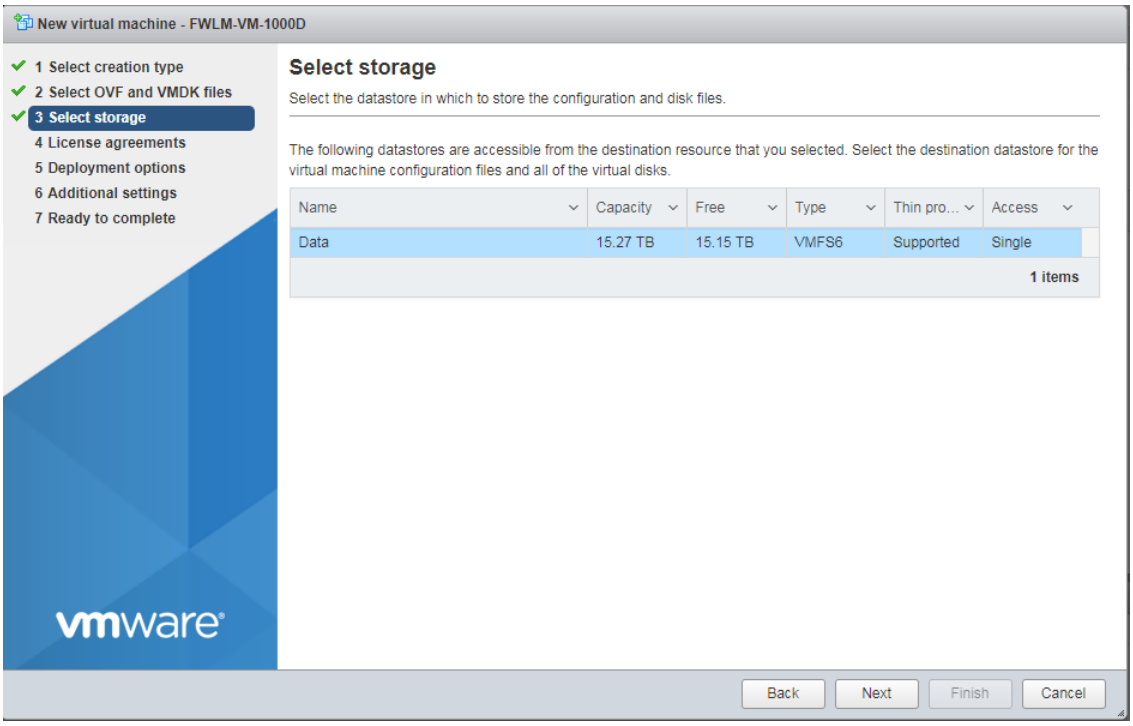
2. Select **Deploy a virtual machine from an OVF or OVA file**. Click **Next**.



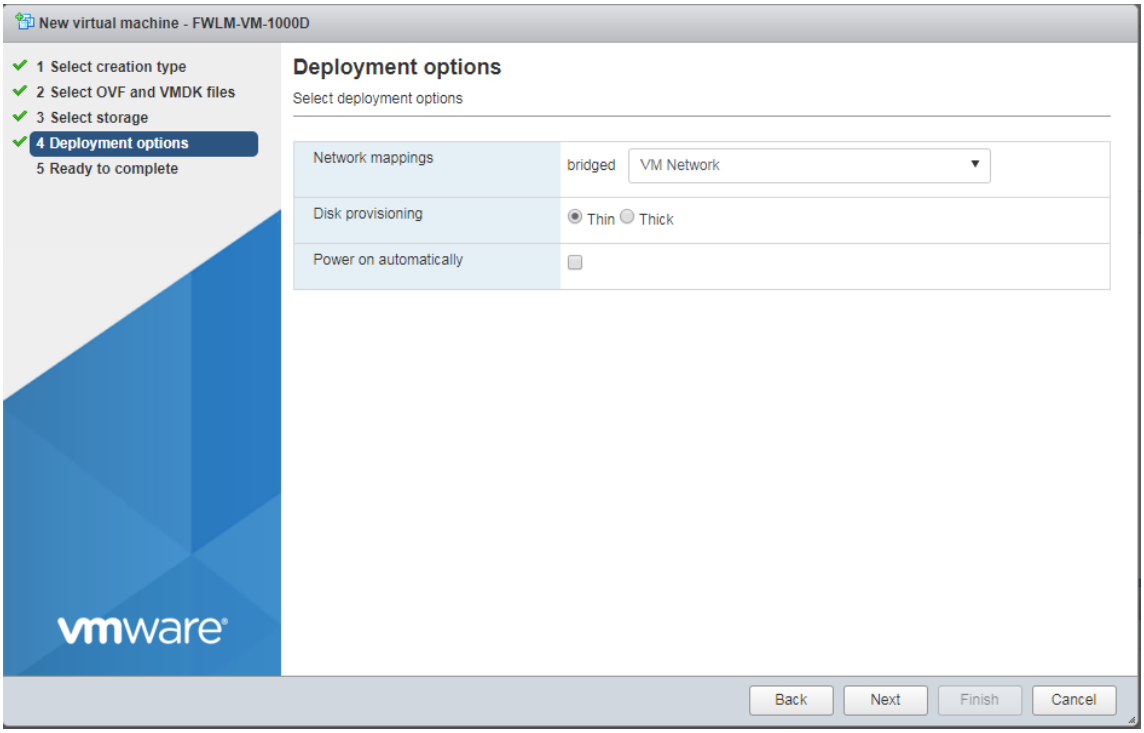
3. Enter a unique name for the virtual machine and click on the space, as indicated, to select or drag and drop the downloaded OVA file. Click **Next**.



4. Select the datastore to store configuration and disk files. Click **Next**.

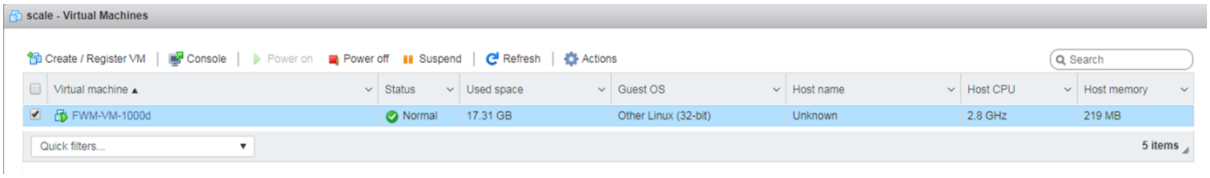


5. The deployment options are displayed. Click **Next**.
6. Select the **Network mappings** as **bridged VM Network**, **Disk provisioning** should be **Thin**. Disable **Power on automatically**. Click **Next**.



7. Review the configured settings and click **Finish**.

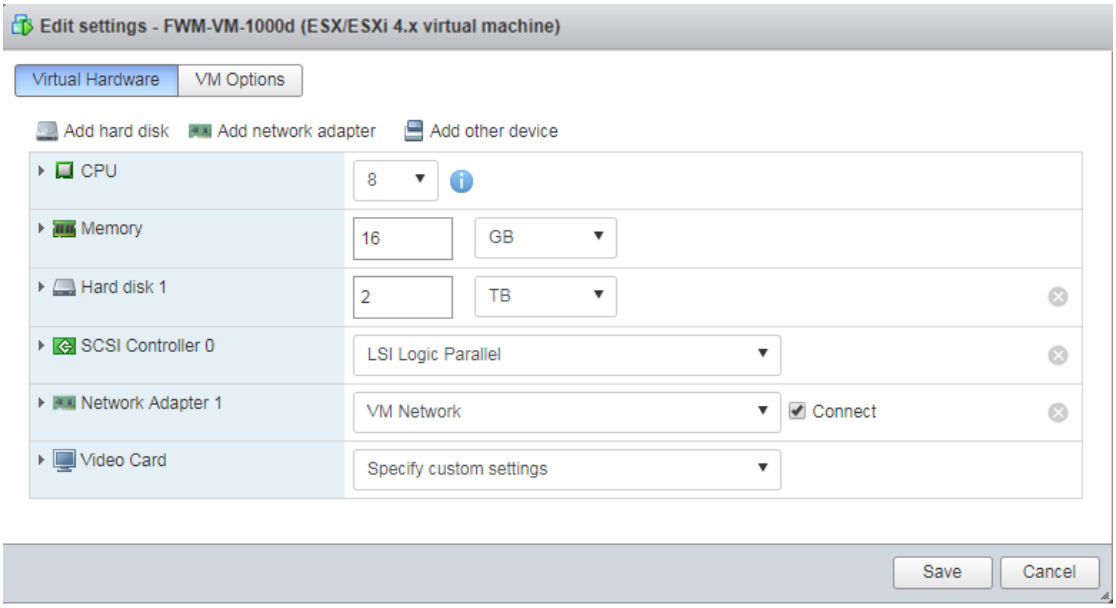
The virtual machine is created.



Configuring the Virtual Machine

After creating a virtual machine, configure it to work as a FWLM-VM-100D or FWLM-VM-1000D. See section Supported Hardware Configuration.

1. Select the listed virtual machine and right-click. Select **Edit settings**.
2. Modify the **CPU** and the **Memory**. Click **Add hard disk** to add a new hard disk. Click **Save**.



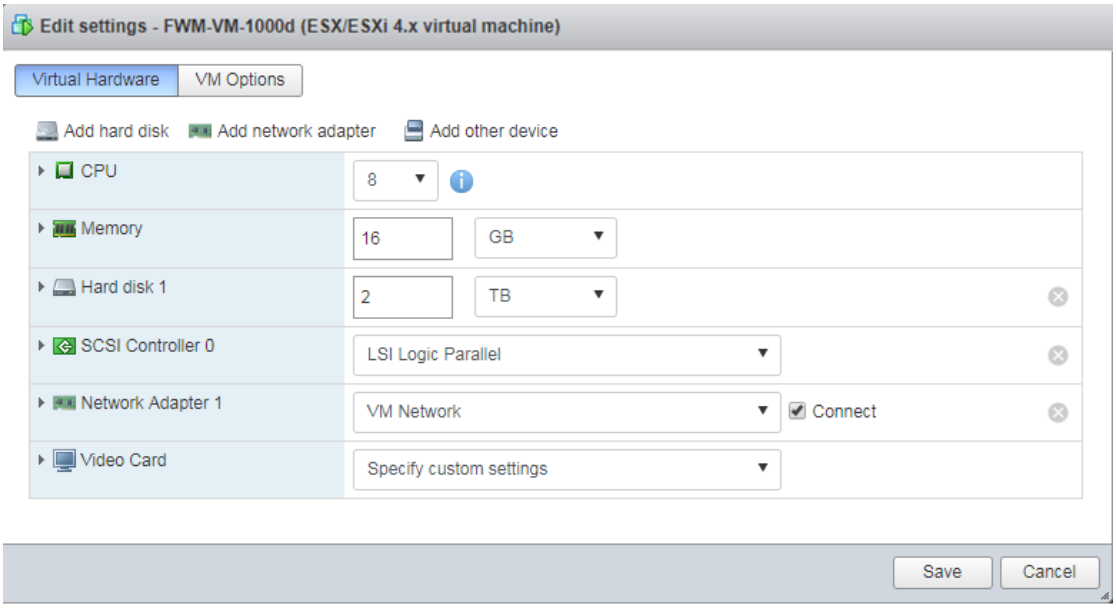
Starting the Virtual Machine

After configuring the newly created virtual machine, select the listed virtual machine and right-click. Select **Power < Power on**.
The Virtual Machine starts.

Expanding the Virtual Hard Disk

You can increase the storage space of a virtual machine by expanding its virtual hard disk. Follow these steps to expand the virtual hard disk.
Note: Decreasing the size of the virtual hard disk is not supported.

1. Run the **resizedisk** command from the IOS CLI to enable resizing the disk.
2. Select the virtual machine on the ESXi console and right click.
3. Select **Power < Power off** to power off the Guest VM.
4. Right click the virtual machine and select **Edit Settings.**
5. Under **Virtual Hardware,** modify the hard disk size (Supported Hardware Configuration)**.**



6. Click **Save.**
7. Right click and select **Power < Power on** to power on the Guest VM.

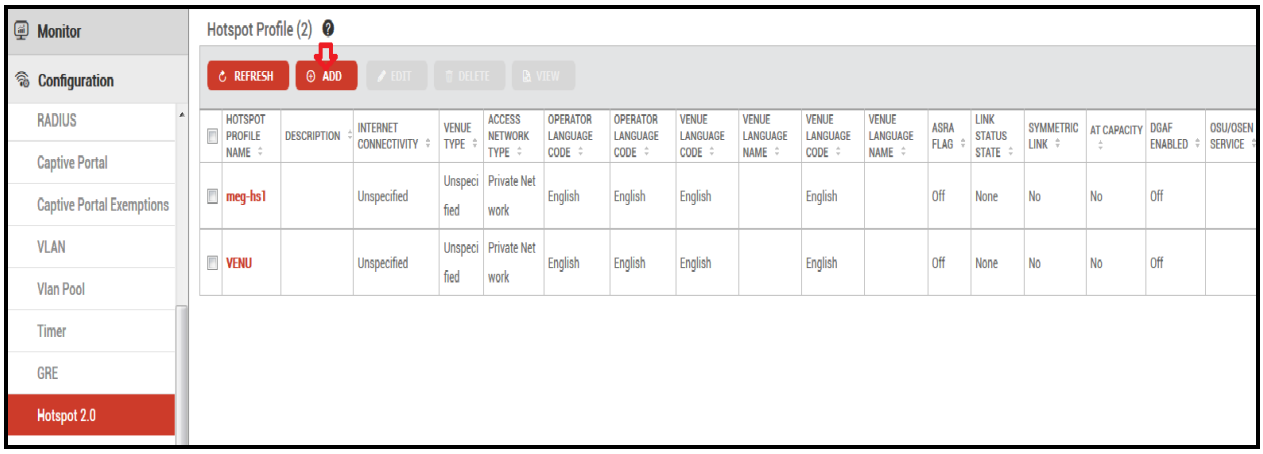
New Features

- Hotspot 2.0 Enhancements
- Spectrum analysis support in FAP
- Beacon Services Enhancements
- Controller Inventory Enhancements

Hotspot 2.0 Enhancements

Hotspot 2.0 is a specification by the Wi-Fi Alliance that specifies a framework for seamless roaming between WiFi networks and Cellular networks. The specification is based on the IEEE802.11u standard; a Generic Advertisement Service (GAS) that provides over-the-air transportation for frames of higher layer advertisements between stations APs and external information servers. This feature will allow users to configure hotspot profiles that can (optionally) be connected to existing ESS Profiles as desired. An ESS-profile connected to a hotspot profile will advertise 802.11u capabilities in its beacons.

The Hotspot Profiles can be created from the **Configuration > Profiles > Hotspot 2.0** page. By default, the page shows the following details about a Hotspot Profile.



Field	Description
Advanced Settings	Provide the following configuration details for advanced settings: • **HESSID -** An AP's Homogenous ESS Identifier (HESSSID), a globally unique identifier, gives a single identifier for a group of APs connected to the same SP or other destination network(s). • **GTK Per Station** - Enables the Group Temporal Key (GTK) to be assigned per station. • **Gas Come Back Flag** - Enables the Generic Advertisement Service (GAS) comeback request/response option. • **Gas Come back Delay (millisecs)** - At the

	end of the GAS comeback delay interval, the client can attempt to retrieve the query response using the comeback request action frame. • **ASRA Flag** - Enable the Additional Step Required for Access (ASRA) to indicate that the network requires one more step for access. • **Authentication type** - Configure the network authentication type required as per ASRA. Supported values are, **Acceptance of terms and conditions, On line enrolment supported, http/https redirection**, and **DNS redirectio**n. • **Redirect URL** - Specify the Redirect URL in case of **http/https redirection** and **DNS Redirectio**n.
WAN Metrics	Provide the following configuration details for WAN metrics: • **Link Status State** - Select the status of the WAN link. • **Symmetric Link** - When enabled, the Up Link Speed configured will be applicable to the Download Link Speed. • **At Capacit**y - Select whether the WAN link is at capacity and no additional mobile devices will be allowed to associate with the AP. • **Down Link speed**/**Up Link speed** - The WAN Backhaul link for current downlink/uplink speed in KBPS. • **Down Link load**/**Up Link load** - The current percentage load of the downlink/uplink connection, measured over an interval the duration of which is reported by the **Load Measurement Duration**. • **Load Measurement Duration** - The duration over which the downlink/uplink load is measured in KBPS.
Connection Capability	The Connection Capability enables filtering of protocols, allowing or restricting traffic on some protocols and ports. A set of system defined protocols as listed. Additionally, you can also create rules for custom protocols.
QoS Map	Create a Quality of Service (QoS) policy by configuring the following DSCP ranges and DSCP exceptions.

	• **DSCP Range**s - For a given DSCP range, specify the User Priority (valid range: 0 - 7), DSCP High Priority (valid range: 0 - 255), and DSCP Low Priority (valid range: 0-255). • **DSCP Exceptions** - For a given DSCP exception, specify the User Priority (valid range: 0 -7) and the DSCP Value (valid range: 0 - 255).
OSU Settings	The Online Sign Up (OSU) Service settings configure one or more hotspot providers offering OSU service. • **Online Sign Up Support** - Select to enable OSU. • **OSEN Enable** - Enable OSU Server-only authenticated layer-2 Encryption Network (OSEN) to indicate that the hotspot uses a OSEN network type. This network provisions clients using the OSU functionality. • **OSU/OSEN ESSID** - Specify the OSU ESSID. • **OSU Server URL** - Specify the URL of the OSU server. • **OSU NAI** - Specify the OSU NAI for authentication. Click Settings to configure the OSU provider settings. • **OSU Provider Friendly Names** • **OSU Provoder Icons** • **OSU Provider Method** - Select one of the OSU provider provisioning methods, **OMA-DM** or **SOAP-XML**. • **OSU Provider Description** - The description of the OSU Provider.

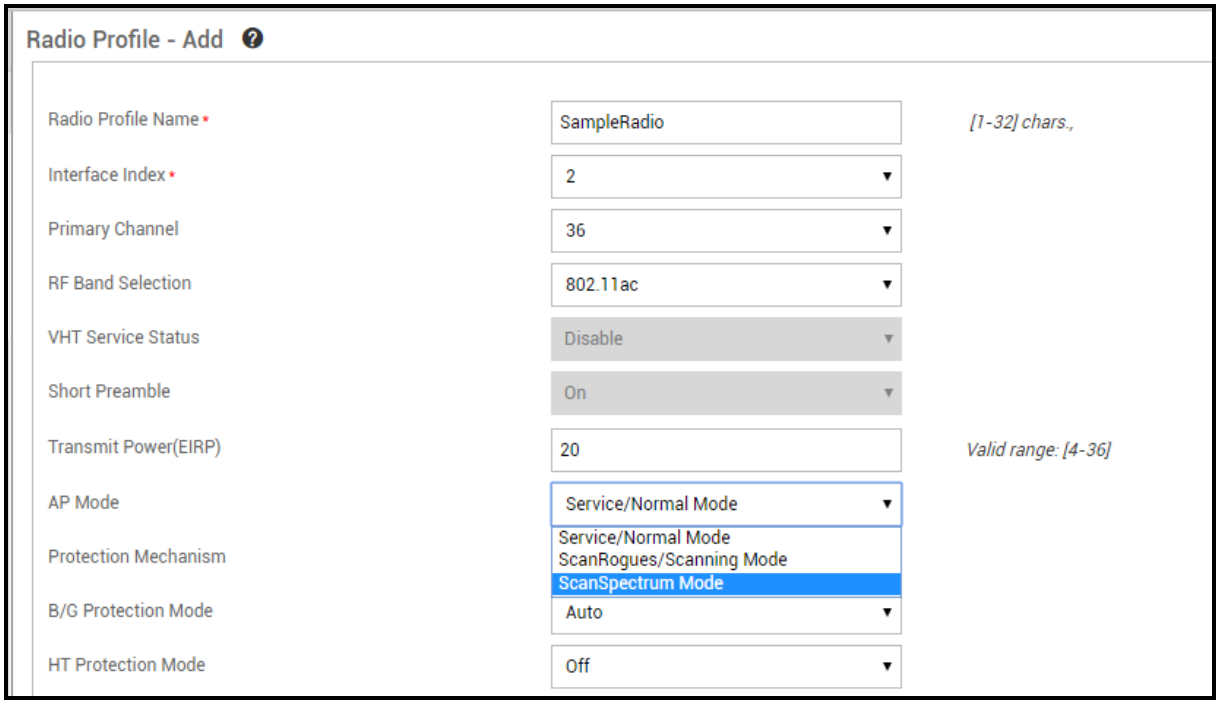
Spectrum analysis support on FAP

This release of FortiWLM introduces Spectrum Analysis support for FAP-U321EV, FAP-U323EV, FAP-U421EV and FAP-U423EV Access Points with Advanced Interference detection mechanism added.
Users can deploy these Access Points (Sensors) in their Wireless network which will scan the environment continuously for Interference and send reports to Spectrum Manager on the Interference detected.
Users are allowed to configure both radios of these sensors in **Scan Spectrum** Mode, which will make the radios to scan the Spectrum.

Enabling Spectrum Analysis

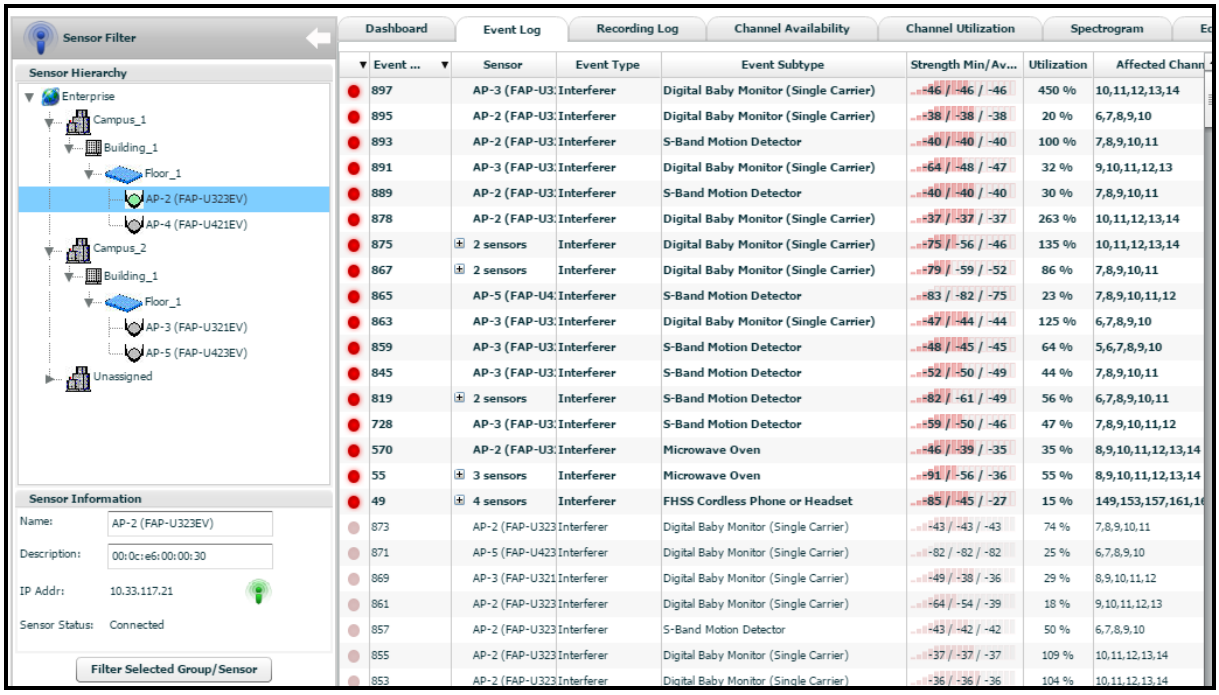
Access Point radios can be configured **Scan Spectrum Mode** using following ways:

1. Add **Radio Profiles** with **AP Mode** as "***ScanSpectrum Mode***"



2. **Create** an **AP Group** with Sensors added into group.
3. **Add** an **AP Template** and **Register** to the AP Group.

Once **Scan Spectrum** is enabled for a particular radio of sensor, sensor starts scanning and reports ***events*** to Spectrum Manager.



Note1: The modification of AP mode from "service mode" to "scan spectrum" mode can be performed by changing the AP Mode from FortiWLC-SD (GUI) or by pushing the AP Template with Radio profile configured "Scan Spectrum" from FortiWLM

Note 2: Users are allowed to configure both radios of FAP-U421EV, FAP-U423EV, FAP-U321EV, FAP-U323EV sensors in ***Scan Spectrum Mode***, which will make the radios to scan both the Radio Spectrum for Interference. For all the other Sensors, Only Single radio can be configured in "*scan spectrum mode*" at a time

Note 3: No Client Service will be provided once radios are in Scan Spectrum Mode

Beacon Services Enhancements

Fortinet Beacon Services use iBeacon to allow mobile application (iOS and Android devices) to receive signals from beacons in the physical world to deliver hyper-contextual content to users based on location. Bluetooth Low Energy (BLE) is the wireless personal area network technology used for transmitting data over short distances. Broadly, the Beacon Service requires a Bluetooth based iBeacon device to broadcast signals and a mobile application to receive these signals once it comes in the configured proximity. You can now create multiple Beacon Service profiles and map APs to a specific profile.

The Beacon services are available by default in FAP U421EV, FAP U423EV, FAP U321EV and FAP U323EV. For other non-wave2 APs, you will need Bluetooth adapters (For example: Broadcom USB Class 2 Bluetooth 4.0 Dongle, CSR 4.0 Bluetooth Dongle and Iogear Bluetooth 4.0 USB Micro Adapter GBU521). Ensure that Bluetooth adapters support Bluetooth version 4.0 or above.

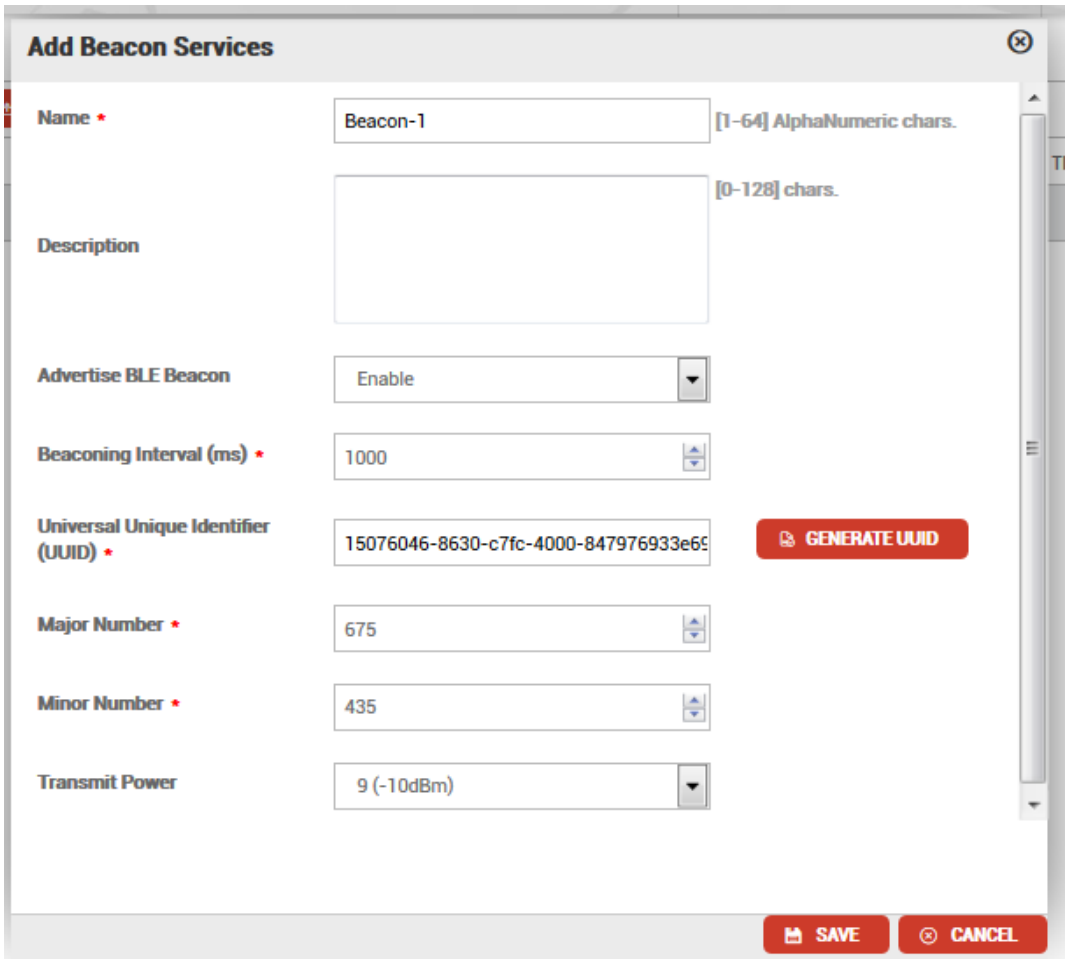
Note: Access points must be connected to 802.3at power supply.

On upgrading the FortiWLM from a previous version to the latest, the existing Beacon profiles in FortiWLM are unregistered from the Controller.

You can perform the following operations to manage the Beacon Services. Navigate to **Configuration > Controller Configuration > Beacon Services**.

Adding Beacon Services Profiles

This option allows you to add a **Beacon Service**. You can create multiple Beacon Service profiles and also map APs to a specific profile.
APs part of a profile send iBeacons that will help advertise hyperlocal content to users in context to their location.



Update the following fields.

- **Name** – Unique name for this **Beacon Service** profile. The supported range is 1-64 alphanumeric characters.
- **Description** – A description of the created Beacon Service. The supported range is 0-128 characters.
- **Advertise BLE Beacon** – Enables the BLE beacons to advertise packets received by devices. These packets determine the location of the device with respect to the Beacon.
- **Beaconing Interval (ms)** – Select the time interval at which the Beacons transmit signals to associated devices, that is, this sets the rate at which beacons advertise packets. Setting the beacon interval to a higher value decreases the frequency of unicasts and broadcasts sent by the AP. The supported range is 100-1000 milliseconds.
- **Universal Unique Identifier (UUID)** – Click **Generate UUID**, to receive a UUID that is specific to the beacon. The purpose of the ID is to distinguish iBeacons in your network from all other beacons in other networks not monitored by you.
- **Major Number** – This number is assigned to some beacons in a network and is used to distinguish this subset of beacons within a larger group of beacons. For example, beacons within a particular geographic area can have the same major number. The supported range is 0 to 65535.
- **Minor Number** – This number is assigned to identify individual beacons. For example, each beacon in a group of beacons with the same major number, will have a unique minor number. The supported range is 0 to 65535.
- **Transmit Power** – Select a power level for the beacon's transmit signal. This higher the power the greater will be the range of your signal. This is measured in dBM (Decibel-Milliwatts). The supported range is 0(-29 dBm) to 15(4dBm).

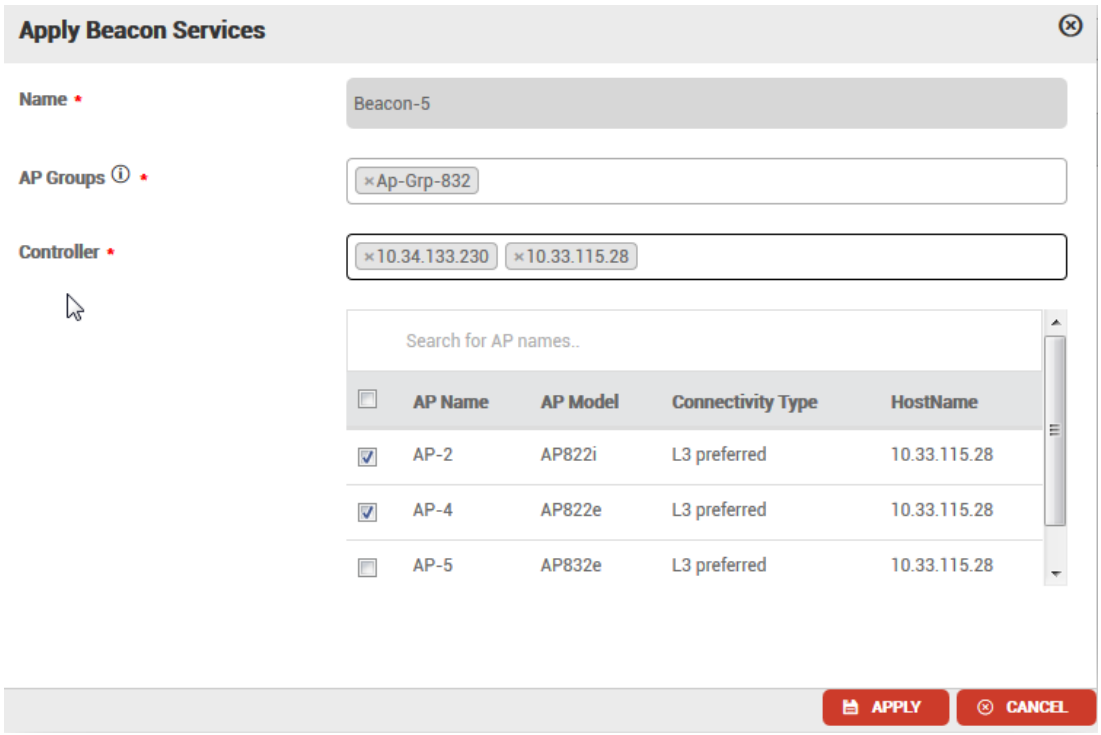
Enabling Beacon Services Profiles

Select the Beacon Services profile and click in the **Action** column to enable the profile.

Applying Beacon Services Profile to APs

Select the **Beacon Services** profile and click in the **Action** column to apply the profile to specific APs. You can apply the profile to all APs of a Controller or to specific APs. These are the supported options:

- **AP Groups** - Select a group from the drop-down list. The profile is pushed only to the APs in the AP Group.
- **Controller** - Select the Controller from the drop-down list and select the supported APs. The profile is pushed to the selected APs.



Note: Controller versions 8.3.0 and above are supported. The list of APs is available only in FortiWLM 8.3.3 and later.

Editing Beacon Services Profiles

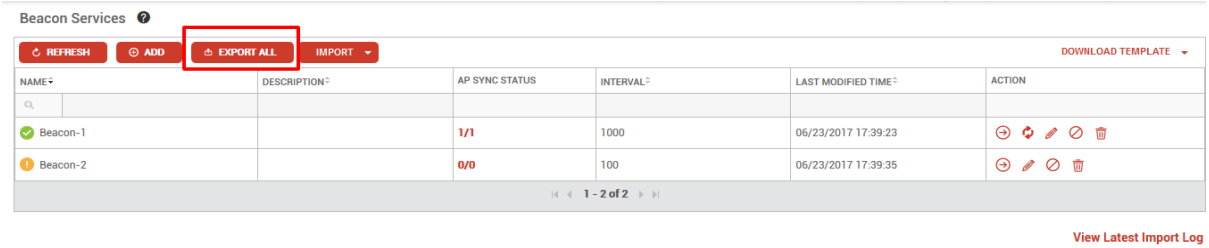
Select the Beacon Services profile and click in the **Action** column to edit the values for an existing profile.

Deleting Beacon Services Profiles

Select the **Beacon Services** profile and click in the **Action** column to delete the profile.

Exporting Beacon Services Profiles

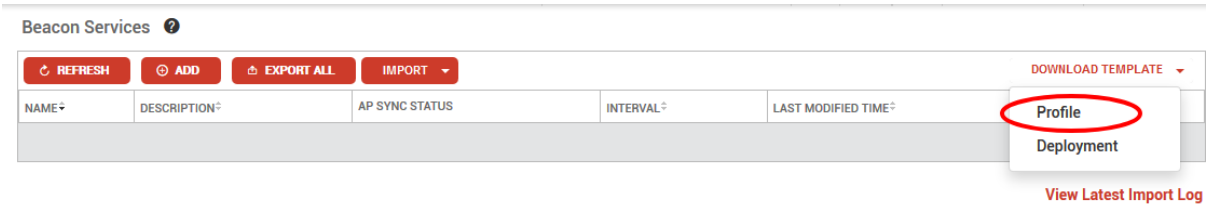
You can export the existing Beacon profiles into your local drive.



Note: The **Export All** option exports the Beacon profiles, but does not export the associated APs.

Importing Beacon Services Profiles

You can load Beacon Services profiles by importing files (*.csv) from your local drive.
Use the **Download Template** option to download the default **Profile** template.

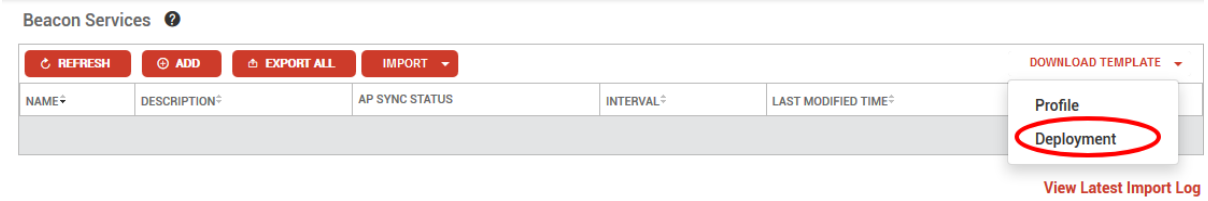


Edit and save these templates.

	A	B	C	D	E	F	G	H
1	name	uniqueidentifier	interval	minornumber	majornumber	descr	blebeacon	transmitpower
2	Beacon-3	545f4426-2896-0785-2c75-97d178e2a613	400	45	56		Enable	-18

Click **Import** and browse to the saved *.csv template file (**Profile** or **Deployment**).

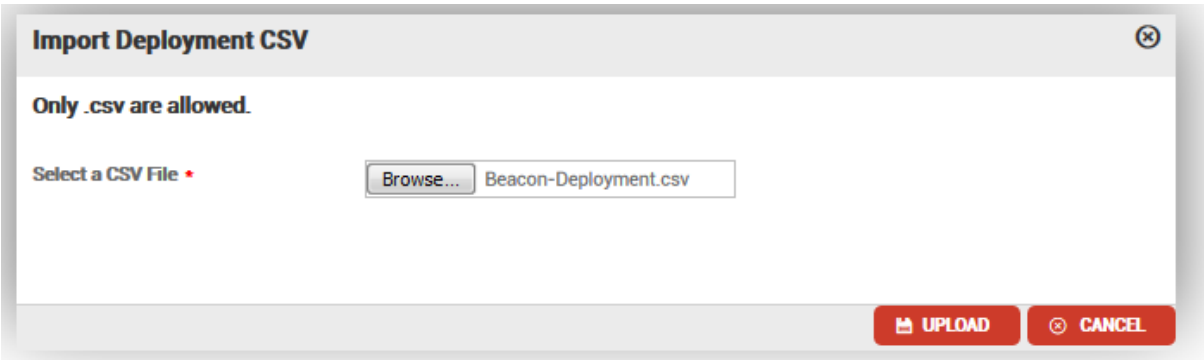
Use the **Download Template** option to download the default **Deployment** template.



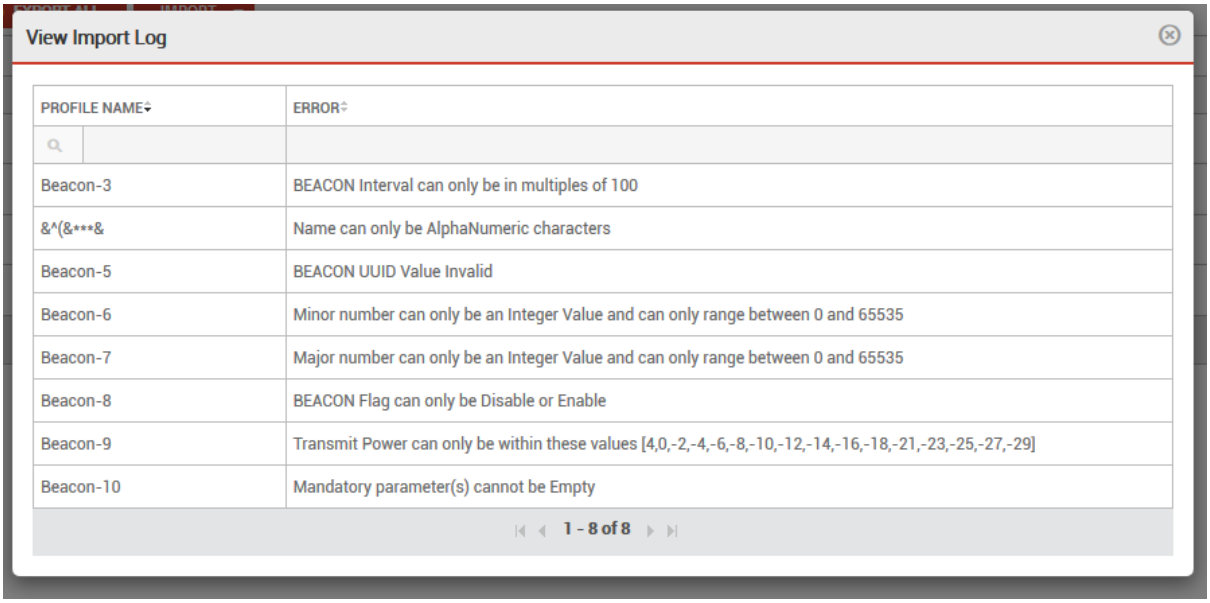
Edit and save the template.

	A	B	C
1	name	controllerId	apId
2	Beacon-2	4	1:2:3

Click **Import** and browse to the saved *.csv template file (**Deployment**).



In case of errors, view the import logs using the **View Latest Import Log** option for error details.



Select the **Apply Beacon Services** option to apply these to the APs.

Controller Inventory Enhancements

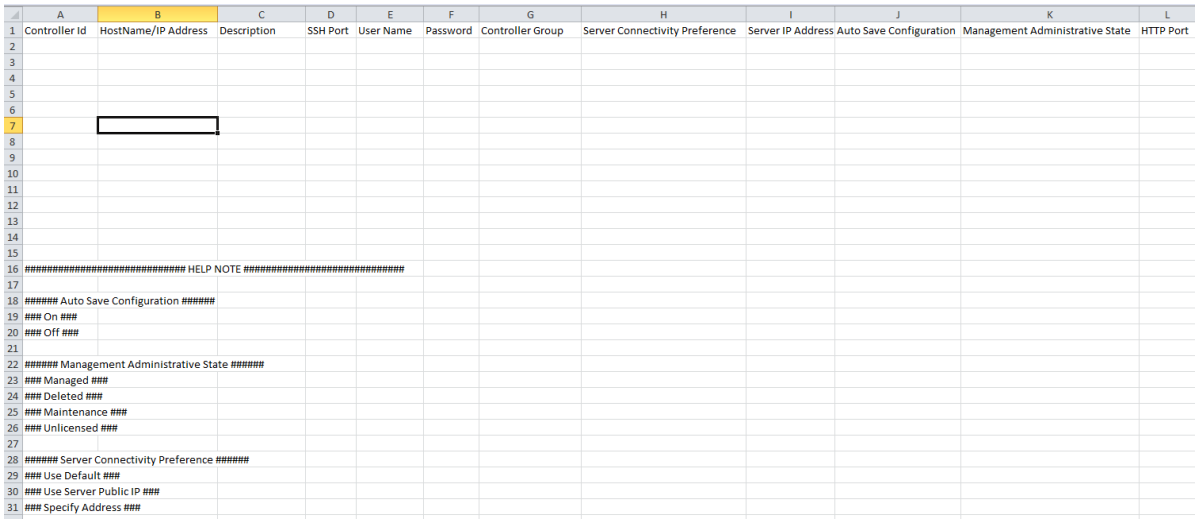
You can add multiple controller entries in Inventory page using IMPORT functionality.

1. Launch the FortiWLM admin UI.
2. Click on **Inventory** and **Controllers** page will be displayed.
3. Click on **DOWNLOAD DEFAULT TEMPLATE** or **EXPORT ALL** button.
4. Download the controller.csv file
5. Open the controller.csv file

Default Template

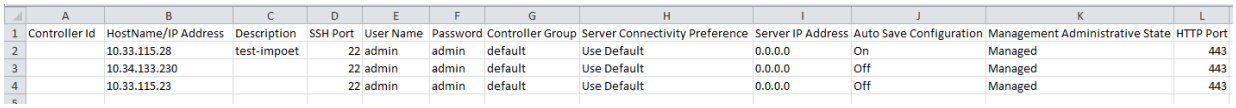
The default template is used as reference template for adding multiple controller entries in the controller.csv file.

1. Launch the FortiWLM admin UI.
2. Click on **Inventory** and **Controllers** page will be displayed.
3. Click on **DOWNLOAD DEFAULT TEMPLATE**.



	A	B	C	D	E	F	G	H	I	J	K	L
1	Controller Id	HostName/IP Address	Description	SSH Port	User Name	Password	Controller Group	Server Connectivity Preference	Server IP Address	Auto Save Configuration	Management Administrative State	HTTP Port
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												
16	########## HELP NOTE ##########											
17												
18	###### Auto Save Configuration ######											
19	### On ###											
20	### Off ###											
21												
22	###### Management Administrative State ######											
23	### Managed ###											
24	### Deleted ###											
25	### Maintenance ###											
26	### Unlicensed ###											
27												
28	###### Server Connectivity Preference ######											
29	### Use Default ###											
30	### Use Server Public IP ###											
31	### Specify Address ###											

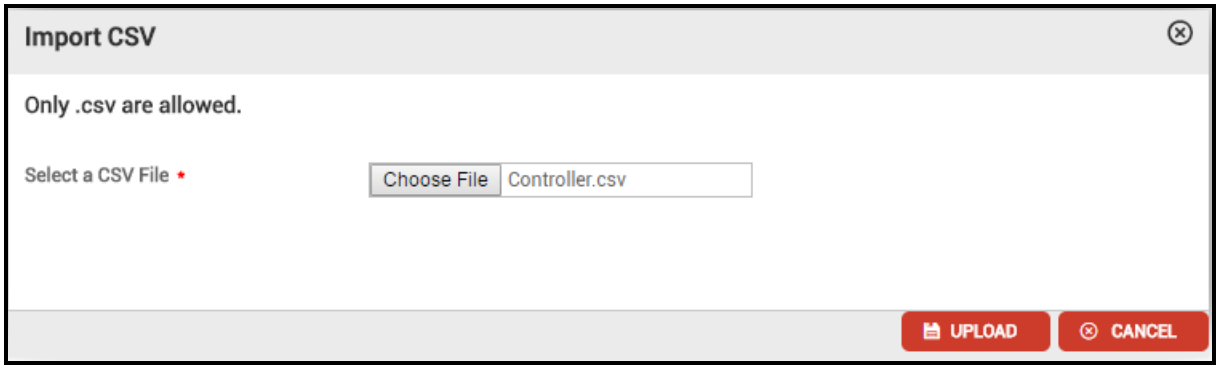
4. Controller.csv file is downloaded in the local drive.
5. Open the file and enter the controller entries.
6. Save the controller.csv file and import the file in Inventory page using IMPORT option.



	A	B	C	D	E	F	G	H	I	J	K	L
1	Controller Id	HostName/IP Address	Description	SSH Port	User Name	Password	Controller Group	Server Connectivity Preference	Server IP Address	Auto Save Configuration	Management Administrative State	HTTP Port
2		10.33.115.28	test-impoet	22	admin	admin	default	Use Default	0.0.0.0	On	Managed	443
3		10.34.133.230		22	admin	admin	default	Use Default	0.0.0.0	Off	Managed	443
4		10.33.115.23		22	admin	admin	default	Use Default	0.0.0.0	Off	Managed	443

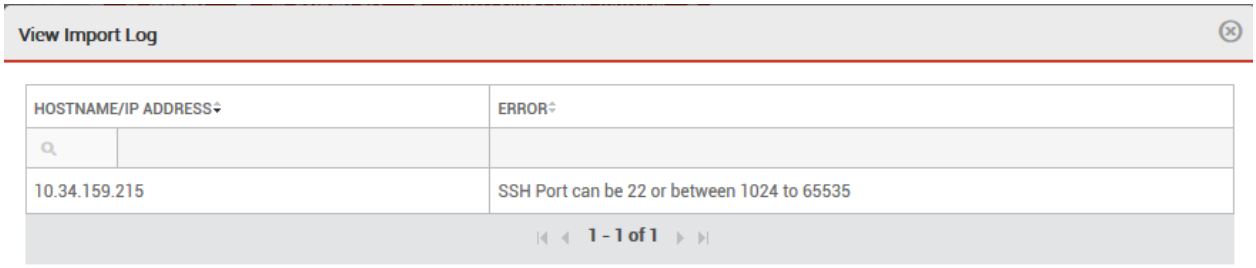
The HostName, User Name, and Password are mandatory fields.

6. Click on **IMPORT** and select the controller.csv file.



7. Click on UPLOAD and controller entry gets added in the Inventory page.

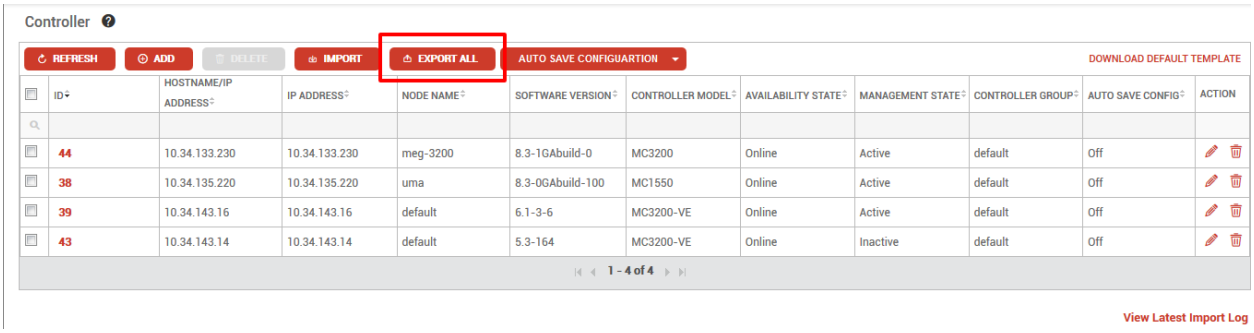
If the import fails, click **View Latest Import Logs** to see the import logs for failure details.



Export Functionality

You can export multiple controller entries to update existing entries using the export functionality.

1. Launch the FortiWLM admin UI.
2. Click on **Inventory** and **Controllers** page will be displayed.
3. Click on **EXPORT ALL** button.



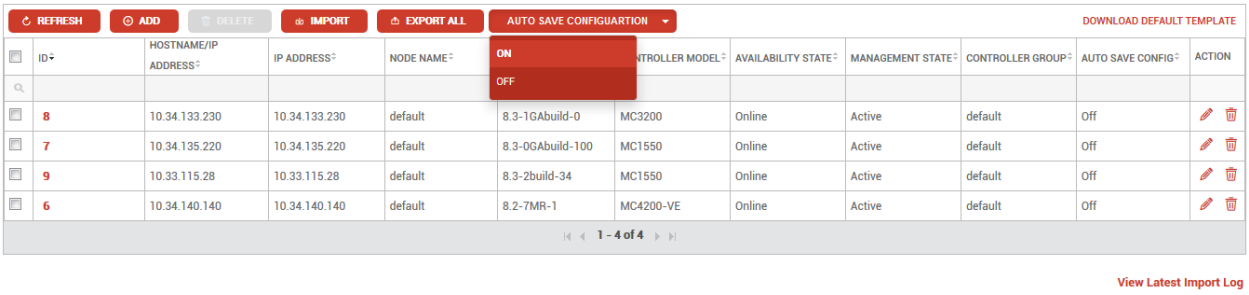
4. Controller.csv will download on your local drive.
5. Controller entries will display in controller csv file.

NOTE: The Controller password will not download from export functionality.
The same file can be edited and imported again.

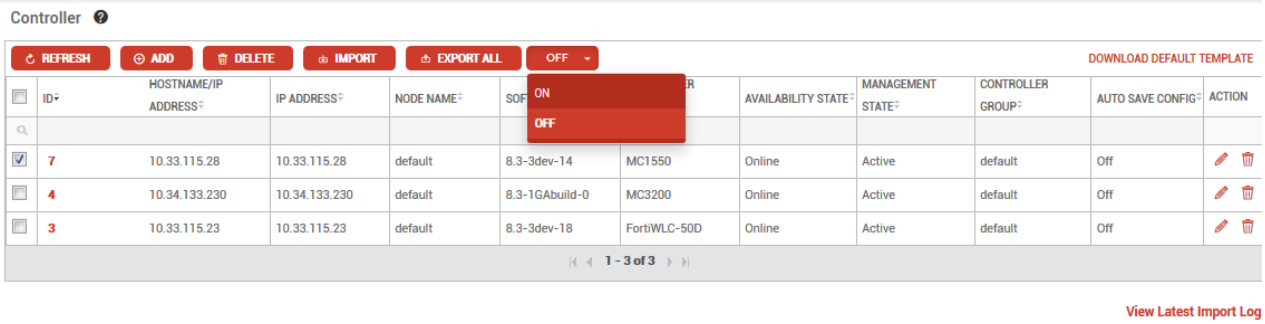
Auto Save Configuration

Auto Save Configuration ON/OFF option is used to apply on multiple/bulk controllers entries in inventory page.

1. Launch the FortiWLM admin UI.
2. Click on **Inventory** and Controllers page will be displayed.
3. Select the controller entry.
4. Select ON from the **Auto Save Configuration** drop down.
5. AUTO SAVE CONFIG column is updated for the controller entry.

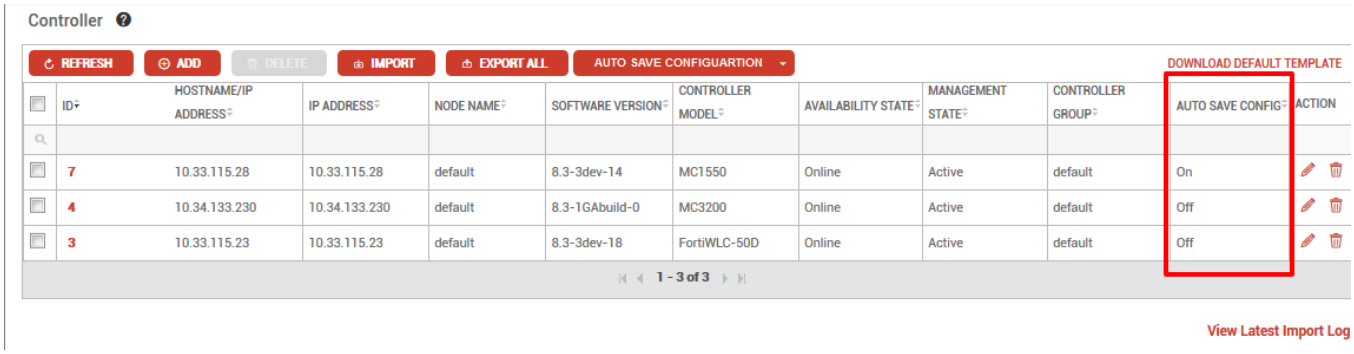


6. Once again select the controller entry.
7. Click on Auto Save Configuration > OFF.
8. **AUTO SAVE CONFIG** column is updated for controller entry.



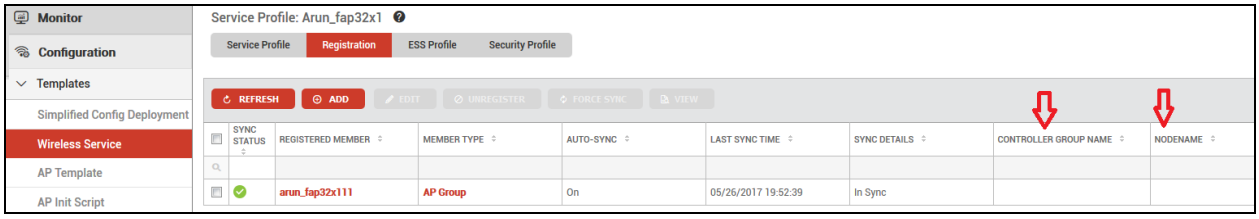
Auto Save Config column added in Inventory Page

1. Launch the FortiWLM admin UI.
2. Click on **Inventory** and **Controller** page will be displayed.
3. Add one controller
4. Auto save config column will display in controller entry.



Controller Group Name and Node Name columns added in Service Profile Registration Page

1. Launch the FortiWLM admin UI.
2. Click on **Inventory** and **Controllers**, Add Controller page will be displayed.
3. Add Controller.
4. Go to Templates.
5. Click on Wireless Service profile.
6. Create a profile and register to the controller.
7. CONTROLLER GROUP NAME and NODENAME column added in Service Profile Registration Page.



Fortinet Universal Access Points

The new Fortinet Universal Access Points (FAP-Us) are dual radio, dual band 802.11ac access points. These access points are designed to provide superior experience in data, voice, and video applications in enterprise class deployments.
For more information on the FAPs, see the corresponding *Quick Start Guides*.

NOTE:
Radio profiles in FortiWLM are not specific to AP models, so to use Wave-2 AP features like 3x3 MIMO and MU-MIMO, create separate radio profiles for FAPs and assign it to an AP group with only FAPs.

FAP-U321EV and FAP-U323EV

FAP-U321EV (indoor) and FAP-U323EV (outdoor) support 3x3 MIMO radios that comply with the IEEE 802.3af and 802.3at PoE specifications.

FAP-U221EV and FAP-U223EV

The FAPs support two 2x2 MIMO radios (band locked) with a single core and comply with the IEEE 802.3af and 802.3at PoE specifications. A maximum of 8 ESS profiles and 128 clients are supported.

FAP-U24JEV

The FAPs support two 1x1 MIMO radios (band locked) with a single core and comply with the IEEE 802.3af and 802.3at PoE specifications. A maximum of 8 ESS profiles and 128 clients are supported. The FAP has one 2x2 radio which will be always configured as two 1x1 interfaces.

FAP-U422EV

The FAP is a Wave-2 access point and supports two 4x4 MIMO radios (band locked) with a dual core. This device complies with the 802.3at PoE specifications. A maximum of 16 ESS profiles are supported. The FAP supports all FortiWLC functionalities same as the FAP-U42xEV.

Fixed Issues

Bug ID	Description
438602	DPI statistics not showing up on the dashboard after replacing the 8.2 database on 8.3.
435093	Unable to pull station activity log from EzRF.
416463	SNMP query on table stops working and throws the genError.
396716	The AP report required to display the correct station count.
371631	The Hyper-V server not reachable after running for more than 3 days with Kernel panic “atkbd.c Spurious ACK on isa0060/serio0”.

Known Issues and Limitations

Bug ID	Description
423760	FWLCVM: Controller discovery in FortiWLM is failing on n+1 failover with auto revert disabled.
414104	Spectrumd crashing continuously when both the Radios of FAP42X have enabled Scan Spectrum Mode.
437402	SAM: Baseline tests are failing for AP1020 and AP832 for RADIUS and WPA2PSK profiles. **Workaround**: Use clear profiles for Baseline tests.
406122	Not able to login to EzRF UI in IE after logout.
438783	Spectrum analysis: Overlay interference is misinterpreted as interference detected by the FAP.

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service